UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/930,903	08/17/2001	Matthew Campagna	F-134	1719

919 7590 10/14/2004

PITNEY BOWES INC.
35 WATERVIEW DRIVE
P.O. BOX 3000
MSC 26-22
SHELTON, CT 06484-8000

EXAMINER	
CHAI, LONGBIT	

ART UNIT	PAPER NUMBER
2131	2

DATE MAILED: 10/14/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/930,903	CAMPAGNA, MATTHEW	
	Examiner	Art Unit	
	Longbit Chai	2131	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *17 August 2001*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☐ Claim(s) _____ is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-36* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *17 August 2001* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

Priority

1. No claim for priority has been made in this application.

2. The effective filing date for the subject matter defined in the pending claims in this application is 8/17/2001.

Claim Objections

3. Claim 21 is objected to because of the following informalities: "described in claim 16" should be changed to "described in claim 20". Appropriate correction is required.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

4. Claims 1, 3 – 5, 27 – 29, 32 – 34 and 36 are rejected under 35 U.S.C. 103(a) as being unpatentable over Gohl (Patent Number: 2002/0099942 A1), hereinafter referred to as Gohl, in view of Fielder (Patent Number: 5963646), hereinafter referred to as Fielder, in view of Kang (Patent Number: US 2001/0016907 A1), hereinafter referred to as Kang, and in view of Scheidt (Patent Number: US 6490680 B1), hereinafter referred to as Scheidt.

5. As per claim 1, 27 – 29, 32 – 34 and 36, Gohl teaches a method for authenticating a message recipient, said method comprising the steps of:

a) generating a password P (Gohl, see for example, Paragraph [0028] Line 16 – 21);

b) sending said password P to said message recipient over a first, secure channel (Gohl, see for example, Paragraph [0028] Line 16 – 21: secured channel is also assured by using SSL secured session layer);

c) generating a first random number as a first initialization vector IV1 (Gohl, see for example, Paragraph [0048] Line 1 – 5 and Line 17 – 21);

d) generating H(IV1|P) as an authentication key AK (Gohl, see for example, Paragraph [0048] Line 1 – 5, Line 17 – 21 and Paragraph [0047] Line 14: The pseudo random string is qualified as a seed, or as a secret, or as a symmetric authentication key);

6. Gohl does not disclose expressly generating an authentication string AS as E(ACNST1, AK), where ACNST1 is a predetermined constant and E is a predetermined symmetric key encryption algorithm.

7. Fielder teaches generating an authentication string AS as E(ACNST1, AK), where ACNST1 is a predetermined constant and E is a predetermined symmetric key encryption algorithm (Fielder, see for example, Column 3 Line 22 – 28).

8. It would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine the teaching of Fielder within the system of Gohl

because Fielder teaches an efficient encryption / decryption method for generating a non-predictable but "deterministic" (or "repeatable") pseudo-random string/seed through a pre-determined constant (Fielder: see for example, Column 3 Line 1 – 3 and Column 3 Line 30 – 32: The pseudo random string is qualified as a seed, or as a secret, or as a symmetric authentication string).

9. Therefore, Gohl as modified teaches:

e) generating an authentication string AS as E(ACNST1, AK), where ACNST1 is a predetermined constant and E is a predetermined symmetric key encryption algorithm (Fielder, see for example, Column 3 Line 22 – 28);

10. Gohl as modified does not teach generating a second random number and receiving a third random number and then further generating an authentication key ARK as H(IV2|IV3|AS)

11. Kang teaches generating a pre- secret / key based on (1) server random number sent, (2) client random number received, and (2) a master secret / key (Kang, see for example, Claim 6 Line 11 – 12: Server random number sent is qualified as IV2, client random number received is qualified as IV3 and a pre-master secret / key / string is qualified as AS).

12. It would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine the teaching of Kang within the system of Gohl as modified because (a) Gohl teaches using SSL (secured session Layer) as the selected security scheme (Gohl, see for example, Paragraph [0028] Line 19 – 21 and Paragraph [0020] Line 1 – 7), and (b) Kang further teaches providing an effective security function

for an enhanced SSL in the application layer to increase the security protection (Kang, see for example, Paragraph [0002] Line 3 – 4).

13. Therefore, Gohl as modified further teaches:

f) generating a second random number as a second initialization vector IV2 (Kang, see for example, Claim 6 Line 11 – 12);

g) sending said vectors IV1 and IV2 to said message recipient over a second channel (Kang, see for example, Claim 6 Line 11 – 12: SSL assures secured channel);

h) receiving a third random number as a third initialization vector IV3 and an authentication response AR from said recipient (Kang, see for example, Claim 6 Line 11 – 12);

i) generating an authentication response key ARK as H(IV2|IV3|AS) (Kang, see for example, Claim 6 Line 11 – 12: a pre-master secret / key / string is qualified as AS and the created master secret / key is equivalent to ARK);

14. Gohl as modified does not disclose expressly authenticating the recipient by encrypting / decrypting a pre-determined constant.

15. Scheidt teaches authenticating the recipient by encrypting / decrypting a pre-determined constant (Scheidt: see for example, Column 13 Line 14 – 16).

16. It would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine the teaching of Scheidt within the system of Gohl as modified because Scheidt teaches a simplified and flexible access for authorized users and maintaining the data security (Scheidt: see for example, Column 1 Line 42 – 47).

j) generating a decryption D(AR, ARK), where D is a symmetric decryption algorithm corresponding to E (Scheidt: see for example, Column 13 Line 14 – 16); and

k) authenticating said message recipient only if D(AR, ARK)=ACNST2, where ACNST2 is a second predetermined constant (Scheidt: see for example, Column 13 Line 14 – 16).

22. As per claim 3, Gohl as modified teaches the claimed invention as described above (see claim 1). Gohl as modified further teaches where H is an encryption algorithm defined hash algorithm using said encryption algorithm E (Gohl: see for example, Paragraph [0047] Line 14).

23. As per claim 4, Gohl as modified teaches the claimed invention as described above (see claim 3). Gohl as modified further teaches said encryption algorithm is expressed in less than 1000 bytes of code; whereby software comprising said algorithm can be quickly downloaded to a user's system (RC4 encryption algorithm is expressed in less than 1000 bytes of code based on Applicant's own admission as well known in the field).

24. As per claim 5, Gohl as modified teaches the claimed invention as described above (see claim 4). Gohl as modified further teaches said encryption algorithm is an RC4 algorithm (RC4 encryption algorithm is well known in the field based on Applicant's own admission).

25. Claim 2 is rejected under 35 U.S.C. 103(a) as being unpatentable over Gohl (Patent Number: 2002/0099942 A1), hereinafter referred to as Gohl, in view of Fielder (Patent Number: 5963646), hereinafter referred to as Fielder, in view of Kang (Patent Number: US 2001/0016907 A1), hereinafter referred to as Kang, in view of Scheidt (Patent Number: US 6490680 B1), hereinafter referred to as Scheidt, and in view of Jevans (Patent Number: US 2001/0055396 A1), hereinafter referred to as Jevans.

26. As per claim 2, Gohl as modified teaches the claimed invention as described above (see claim 1). Gohl as modified further teaches a) steps a through f are carried out by a sender; b) said sender sends said vector IV1 to said message recipient through a server, said server sending said vector IV1 and said vector IV2 to said message recipient; and c) said server receives said vector IV3 and said response AR from said recipient, and carries out steps i through k to authenticate said recipient (See the same rationale as above in rejecting the claim 1).

27. However, Gohl as modified teaches said server sending vector IV1 and vector IV2 to message recipient but does not disclose expressly that said server sending vector IV1 together with vector IV2 to message recipient in this claim limitation (b).

28. Jevans teaches allowing a list of security sensitive information to be sent simultaneously by the sender (Jevans: see for example, Paragraph [0021] Line 10 – 12).

29. It would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine the teaching of Jevans within the system of Gohl

because Jevans teaches a method of transmitting the documents / messages securely and efficiently (Jevans: see for example, Paragraph [0003] Line 2 – 4).

30. Claims 6 – 7 are rejected under 35 U.S.C. 103(a) as being unpatentable over Gohl (Patent Number: 2002/0099942 A1), hereinafter referred to as Gohl, in view of Sandhu (Patent Number: 2002/0078353 A1), hereinafter referred to as Sandhu.

31. As per claim 6, Gohl teaches a method for sending an encrypted message, said method comprising the steps of:

a) generating a random number as an initialization vector IV4 (Gohl: see for example, Claim 11 Line 5 – 8);

b) generating a private key PK as H(IV4|P), where P is a password known to a message recipient (Gohl: see for example, Claim 11 Line 5 – 8 and Paragraph [0048] Line 3 – 5: The pseudo random string is qualified as a seed, or as a secret, or as a symmetric encryption key);

32. Gohl does not teach message authentication by using E(M | H(M), PK).

33. Sandhu teaches ENC=E(M | H(M), PK), M is said message, and E is a predetermined encryption algorithm (Sandhu: see for example, Paragraph [0009] Line 5 – 12).

34. It would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine the teaching of Sandhu within the system of Gohl

because Sandhu teaches enhanced high security cryptosystem especially for message authentications (Sandhu: see for example, Paragraph [0001] and [0009] Line 5 – 12).

c) generating an encryption ENC=E(M | H(M), PK), where E is a predetermined symmetric key encryption algorithm (Sandhu: see for example, Paragraph [0009] Line 8 – 12);

d) sending (IV4, ENC) to said message recipient (Gohl: see for example, Claim 11 Line 5 – 8) & (Sandhu: see for example, Paragraph [0009] Line 8 – 12);

35. As per claim 7, Gohl as modified teaches the claimed invention as described above (see claim 6). Gohl as modified further teaches receiving authentication of said message recipient prior to sending (IV4, ENC) (Gohl: see for example, Paragraph [0006] Line 10).

36. Claims 2 – 5 and 8 – 12 are rejected under 35 U.S.C. 103(a) as being unpatentable over Gohl (Patent Number: 2002/0099942 A1), hereinafter referred to as Gohl, in view of Sandhu (Patent Number: 2002/0078353 A1), hereinafter referred to as Sandhu, in view of Fielder (Patent Number: 5963646), hereinafter referred to as Fielder, in view of Kang (Patent Number: US 2001/0016907 A1), hereinafter referred to as Kang, and in view of Scheidt (Patent Number: US 6490680 B1), hereinafter referred to as Scheidt.

37. As per claim 8, Gohl as modified teaches the claimed invention as described above (see claim 7). Gohl as modified further teaches said message recipient is authenticated by the steps of:

38. a) generating a password P (Gohl, see for example, Paragraph [0028] Line 16 – 21);

39. b) sending said password P to said message recipient over a first, secure channel (Gohl, see for example, Paragraph [0028] Line 16 – 21: secured channel is also assured by using SSL secured session layer);

40. c) generating a first random number as a first initialization vector IV1 (Gohl, see for example, Paragraph [0048] Line 1 – 5 and Line 17 – 21);

41. d) generating H(IV1|P) as an authentication key AK (Gohl, see for example, Paragraph [0048] Line 1 – 5 and Line 17 – 21: The pseudo random string is qualified as a seed, or as a secret, or as a symmetric authentication key);

42. Gohl does not disclose expressly generating an authentication string AS as E(ACNST1, AK), where ACNST1 is a predetermined constant and E is a predetermined symmetric key encryption algorithm.

43. Fielder teaches generating an authentication string AS as E(ACNST1, AK), where ACNST1 is a predetermined constant and E is a predetermined symmetric key encryption algorithm (Fielder, see for example, Column 3 Line 22 – 28).

44. It would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine the teaching of Fielder within the system of Gohl because Fielder teaches an efficient encryption / decryption method for generating a

non-predictable but "deterministic" (or "repeatable") pseudo-random string/seed through a pre-determined constant (Fielder: see for example, Column 3 Line 1 – 3 and Column 3 Line 30 – 32: The pseudo random string is qualified as a seed, or as a secret, or as a symmetric authentication string).

45. Therefore, Gohl as modified teaches:

46. e) generating an authentication string AS as E(ACNST1, AK), where ACNST1 is a predetermined constant and E is a predetermined symmetric key encryption algorithm (Fielder, see for example, Column 3 Line 22 – 28);

47. Gohl as modified does not teach generating a second random number and receiving a third random number and then further generating an authentication key ARK as H(IV2|IV3|AS)

48. Kang teaches generating a pre- secret / key based on (1) server random number sent, (2) client random number received, and (2) a master secret / key (Kang, see for example, Claim 6 Line 11 – 12: Server random number sent is qualified as IV2, client random number received is qualified as IV3 and a pre-master secret / key / string is qualified as AS).

49. It would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine the teaching of Kang within the system of Gohl as modified because (a) Gohl teaches using SSL (secured session Layer) as the selected security scheme (Gohl, see for example, Paragraph [0028] Line 19 – 21 and Paragraph [0020] Line 1 – 7), and (b) Kang further teaches providing an effective security function

for an enhanced SSL in the application layer to increase the security protection (Kang, see for example, Paragraph [0002] Line 3 – 4).

50. Therefore, Gohl as modified further teaches:

51. f) generating a second random number as a second initialization vector IV2 (Kang, see for example, Claim 6 Line 11 – 12);

52. g) sending said vectors IV1 and IV2 to said message recipient over a second channel (Kang, see for example, Claim 6 Line 11 – 12: SSL assures secured channel);

53. h) receiving a third random number as a third initialization vector IV3 and an authentication response AR from said recipient (Kang, see for example, Claim 6 Line 11 – 12);

54. i) generating an authentication response key ARK as H(IV2|IV3|AS) (Kang, see for example, Claim 6 Line 11 – 12: a pre-master secret / key / string is qualified as AS and the created master secret / key is equivalent to ARK);

55. Gohl as modified does not disclose expressly authenticating the recipient by encrypting / decrypting a pre-determined constant.

56. Scheidt teaches authenticating the recipient by encrypting / decrypting a pre-determined constant (Scheidt: see for example, Column 13 Line 14 – 16).

57. It would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine the teaching of Scheidt within the system of Gohl as modified because Scheidt teaches a simplified and flexible access for authorized users and maintaining the data security (Scheidt: see for example, Column 1 Line 42 – 47).

58. j) generating a decryption D(AR, ARK), where D is a symmetric decryption algorithm corresponding to E (Scheidt: see for example, Column 13 Line 14 – 16); and

59. k) authenticating said message recipient only if D(AR, ARK)=ACNST2, where ACNST2 is a second predetermined constant (Scheidt: see for example, Column 13 Line 14 – 16).

60. As per claim 9, Gohl as modified teaches the claimed invention as described above (see claim 8). Gohl as modified further teaches a) steps a through f are carried out by a sender; b) said sender sends said vectors IV1 and IV2 to said message recipient through a server; and c) said server receives said vector IV3 and said response AR from said recipient, and carries out steps i through k to authenticate said recipient (See the same rationale as above in rejecting the claim 8).

61. As per claim 10, Gohl as modified teaches the claimed invention as described above (see claim 6). Gohl as modified further teaches where H is an encryption algorithm defined hash algorithm using said encryption algorithm E (Gohl: see for example, Paragraph [0047] Line 14).

62. As per claim 11, Gohl as modified teaches the claimed invention as described above (see claim 10). Gohl as modified further teaches said encryption algorithm is expressed in less than 1000 bytes of code; whereby software comprising said algorithm can be quickly downloaded to a user's system (Sandhu: see for example, Paragraph [0008] Line 8 – 10: RC4 encryption algorithm is expressed in less than 1000 bytes of code based on Applicant's own admission as well known in the field).

63. As per claim 12, Gohl as modified teaches the claimed invention as described above (see claim 11). Gohl as modified further teaches said encryption algorithm is an RC4 algorithm (RC4 encryption algorithm is well known in the field based on Applicant's own admission) & (Sandhu: see for example, Paragraph [0008] Line 8 – 10).

64. Claims 18, 19, 20 – 22, 30, 31 and 35 are rejected under 35 U.S.C. 103(a) as being unpatentable over Gohl (Patent Number: 2002/0099942 A1), hereinafter referred to as Gohl, in view of Sandhu (Patent Number: 2002/0078353 A1), hereinafter referred to as Sandhu.

65. As per claim 18, 30, 31 and 35, Gohl teaches method for receiving an encrypted message, said method comprising the steps of:

a) receiving (IV4, ENC), where ENC=E(M|H(M), PK), M is said message, and E is a predetermined encryption algorithm (Gohl: see for example, Claim 11 Line 5 – 8);

66. Gohl does not teach message authentication by using E(M|H(M), PK).

67. Sandhu teaches ENC=E(M|H(M), PK), M is said message, and E is a predetermined encryption algorithm (Sandhu: see for example, Paragraph [0009] Line 5 – 12).

68. It would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine the teaching of Sandhu within the system of Gohl because Sandhu teaches enhanced high security cryptosystem especially for message authentications (Sandhu: see for example, Paragraph [0001] and [0009] Line 5 – 12).

b) generating PK as H(IV4 | P), where P is a password received from a sender of said message over a secure channel (Gohl: see for example, Claim 11 Line 5 – 8 and Paragraph [0048] Line 3 – 5: The pseudo random string is qualified as a seed, or as a secret, or as a symmetric encryption key);

c) generating D(ENC, PK)=(M|H(M)), where D is a symmetric key decryption algorithm corresponding to E (Sandhu: see for example, Paragraph [0009] Line 8 – 12);

d) calculating H(M) from said value of M generated in step c (Sandhu: see for example, Paragraph [0009] Line 8 – 12); and

e) accepting said generated value of M only if said calculated value of H(M) equals said value of H(M) generated in step c (Sandhu: see for example, Paragraph [0009] Line 8 – 12).

69. As per claim 19, Gohl as modified teaches the claimed invention as described above (see claim 18). Gohl as modified further teaches where H is an encryption algorithm defined hash algorithm using said encryption algorithm E (Sandhu: see for example, Paragraph [0009] Line 5 – 12).

70. As per claim 20, Gohl as modified teaches the claimed invention as described above (see claim 19). Gohl as modified further teaches said encryption algorithm is expressed in less than 1000 bytes of code; whereby software comprising said algorithm can be quickly downloaded to a user's system (Sandhu: see for example, Paragraph [0008] Line 8 – 10: RC4 encryption algorithm is expressed in less than 1000 bytes of code based on Applicant's own admission as well known in the field).

71. As per claim 21, Gohl as modified teaches the claimed invention as described above (see claim 20). Gohl as modified further teaches said encryption algorithm is an RC4 algorithm (RC4 encryption algorithm is well known in the field based on Applicant's own admission) & (Sandhu: see for example, Paragraph [0008] Line 8 – 10).

72. As per claim 22, Gohl as modified teaches the claimed invention as described above (see claim 18). Gohl as modified further teaches said initialization vector IV4 and said encryption ENC are received from said sender through a server (Gohl: see for example, Claim 11 Line 5 – 8 and Paragraph [0048] Line 3 – 5).

73. As per claim 13 – 17, the claims 13 – 17 does not further teach over claim 1 – 5 and thereby see same rationale addressed above in rejecting claims 1 – 5.

74. As per claim 23 – 26, claims 23 – 26 do not further teach over claims 1 – 5. Therefore, see same rationale addressed above in rejecting claims 1 – 5.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Longbit Chai whose telephone number is 703-305-0710. The examiner can normally be reached on Monday-Friday 8:00am-5:00pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz R Sheikh can be reached on 703-305-9648. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Longbit Chai
Examiner
Art Unit 2131

LBC

AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100